RISK MANAGEMENT POLICY
PI-COR-RCI-001 - REVISION 03. DATE: 08/11/2026

Rua Hungria, 1400, 5th floor, Jardim Europa,
Postal Code: 01455-000, São Paulo – SP
(11) 3500- 8600 igua.com.br

1 OBJECTIVE

To establish guidelines and competencies for risk management, enabling the identification, assessment, prioritization, treatment, communication, and monitoring of business risks. The policy also aims to promote and encourage a risk culture within the Company.

2 REFERENCES

- Corporate Governance Rules of the Company's Articles of Association;
- IBGC (Brazilian Institute of Corporate Governance);
- ABNT NBR ISO 31001 – Risk Management;
- ABNT NBR ISO 37001 – Anti-bribery Management Systems - Requirements;
- ABNT NBR ISO 37301 – Compliance Management Systems - Requirements;
- COSO ERM (Enterprise Risk Management);
- COSO ICIF (Internal Control – Integrated Framework);
- COBIT (Control Objectives for Information and Related Technology);
- PI-COR-CPL-009 - Compliance Policy;
- PI-COR-RCI-002 - Approval Levels and Authority Delegation Policy;
- PI-COR-RCI-003 - Crisis Management Policy.

3 SCOPE

This policy applies to all employees and third parties of the Iguá Saneamento Group.

4 TERMS AND DEFINITIONS

- **Risk appetite** : The maximum level to which the Company is willing to expose itself in relation to risk(s) in order to achieve its strategic objectives.
- **CA** : Board of Directors of Iguá Saneamento.
- **CAE** : Statutory Audit Committee.
- **COBIT** : Control Objectives for Information and Technology. A guide or set of best practices on enterprise information technology governance.
- **Compliance :** Adherence to regulations, laws (tax, labor **,** environmental and other applicable to the Company), *covenants* , contracts and internal rules, procedures, guidelines and policies

that apply to the business.

- **Internal Controls:** Internal control is a process conducted by the entity's governance structure, management, and other professionals, and designed to provide reasonable assurance regarding the achievement of objectives related to operations, disclosure, and compliance.
- **COSO** : *The Committee of Sponsoring Organizations* is a private, non-profit organization created to prevent and avoid fraud in the Company's internal procedures and processes through ethics, effective internal controls, and corporate governance.
    - **COSO ERM:** Assesses risk exposure in relation to the company's strategic objectives.
    - **COSO ICIF:** Evaluates the effectiveness of the internal control system in mitigating risks.
- **Risk Owner** : Person or area responsible for identifying, assessing, treating, monitoring, and reporting a specific risk, ensuring the implementation and effectiveness of mitigation actions, as well as the alignment of the risk with strategic objectives, internal policies, and the Company's Risk Appetite.
- **Risk Appetite Statement (RAS)** : A formal declaration that defines the limits of risk exposure acceptable to the Company, guiding the assessment, treatment, and escalation of risks in alignment with its strategy and governance.

5 GENERAL GUIDELINES (RISK MANAGEMENT)

5.1.1 The Risk Management function is a cyclical and dynamic process that identifies, assesses, monitors, and responds to risks that may compromise the achievement of the Company's strategic objectives or cause significant impacts on its business. This process allows decision-makers at all levels to have timely access to sufficient information related to the risks to which they are exposed,

in order to support decisions and the definition of strategies that increase the likelihood of achieving objectives and minimize risks to acceptable levels.

5.1.2 This is a preventative approach that aims to create ways to manage and keep risks under control (within the established risk appetite) in order to anticipate potential incidents or crises.

5.1.3 There are two distinct and complementary views of risk management: Corporate View and Transactional View.

Corporate Vision manages risks that affect the Company as a whole and are directly related to the Company's strategic objectives and business continuity, including external risks.

The Transactional View (operational layer) manages risks related to the Company's processes, systems, contracts, and business units, considering the specific impact on each area. This type of risk details and complements corporate risks, being associated with them as risk factors, as illustrated below:

Figure 01: Distinct Views of Risk Management

5.1.4 Risk management is directly related to sustainable growth, profitability, preservation, and the creation of value for the company and its shareholders,

since this process allows for the identification not only of threats but also of business opportunities.

5.1.5 An effective risk management process, achieved through adherence to good Corporate Governance practices, aims to manage risks effectively, allowing those responsible at all levels of governance to have timely access to sufficient information related to the risks to which they are exposed, in order to support decisions and the definition of strategies that increase the likelihood of achieving objectives and minimize risks to acceptable levels.

5.1.6 Risk management, through a structured approach and a better understanding of the interrelationships between risks, aligns strategy, processes, people, technology, and knowledge, leveraging the benefits inherent in diversification, aiming to preserve and create value for the company.

5.1.7 With the goal of standardizing Risk Management at Iguá, it is established that:

- Risk management should be embedded in the company's culture, being present in all processes and activities.
- Leadership must promote a risk management culture at all hierarchical levels and in their respective areas of operation, as well as ensure the application of principles and adherence to risk management procedures.
- Senior Management sets the tone for the entire company, reinforcing the importance and establishing supervisory responsibilities for risk management.
- Risk-based decision-making should be incorporated into management, aiming at preserving and creating value for the company.
- Risk management should be integrated into the processes of Management, Compliance, Internal Controls and Internal Audit, promoting the early identification of risks and their conservative and timely management.
- Independence in the risk management process and segregation of duties between risk-takers and those responsible for monitoring risks must be ensured.
- Continuous risk monitoring and its incorporation into routine management are vital to ensuring the effectiveness of risk management and its improvement through frequent evaluation cycles and reviews, aiming at continuous process improvement.
- The analyses, responses, and approvals of **corporate risks** , after validation of their criticality, must be presented to the levels, according to the Company's Approval Authority Table, being ALC-RCI-3 - Validation/Approval of Corporate Risks.

- The analyses, responses, and approvals of **transactional risks** , after validation of their criticality, must be presented to the levels according to the Company's Approval Level Table, being ALC-RCI-4 - Transactional Risk Validation/Approval :
- The Audit Committee and the Board of Directors must be periodically informed about the risks identified in the **Corporate Risk Matrix** , ensuring full knowledge and monitoring of relevant exposures, in accordance with the Company's strategy and risk appetite.

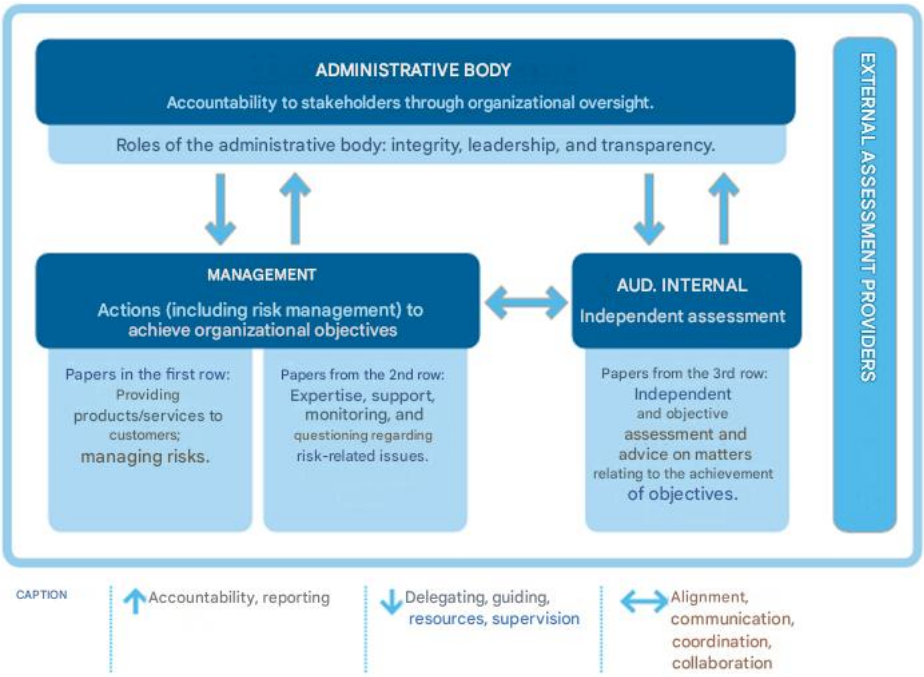
6 STRATEGIC ALIGNMENT AND INTEGRATED MODEL

6.1.1 Risk management is an integral part of the process of developing strategic objectives and is directly aligned with these objectives, establishing an integrated and virtuous feedback loop between the Company's lines of defense for broader coverage of internal and external risk factors in relation to expected results.

6.1.2 The risk management framework supports the integration of governance at all levels, activities, and significant functions, encompassing diverse areas and specialties, working synergistically to protect the business and support leadership in monitoring and promptly adapting its strategy to potential changes in the risk environment.

Iguá Saneamento's methodological approach is based on the integrated framework suggested by COSO and the guidelines defined in ISO 31000 for Risk Management, also observing the concepts established in the Three Lines Model, developed by the IIA, which is illustrated below in Figure 2.

Figure 02: Three Lines of Defense Model IIA



The Three Lines of Defense Model, as established by the Institute of Internal Auditors (IIA) define a governance structure that ensures the proper segregation of responsibilities in risk management. In this model, the **First Line** (business areas) is responsible for the direct management of risks and decision-making, the **Second Line** (Compliance, Risk and Internal Controls Management) exercises independent oversight, establishes methodologies and policies, and monitors the Risk Management Matrix, and the **Third Line** (Internal Audit) provides independent and objective assurance on the effectiveness of risk management, internal controls, and governance processes.

7 RISK APPETITE (RAS)

Risk Appetite The Statement (RAS) represents the formal declaration, approved by the Board of Directors, that defines the level and type of risks the Company is willing to assume in conducting its activities, with a view to achieving its operational, financial, regulatory and sustainability objectives.

Risk appetite guides decision-making, prioritization of initiatives, allocation of resources, and monitoring of corporate risks, and should be permanently aligned with the company's strategy, response capacity, and applicable regulatory requirements.

The definition, operationalization, monitoring, and review of Risk Appetite are detailed in PR-COR-RCI-004 – Risk Appetite Procedure, which establishes the methodological guidelines, roles and responsibilities, tolerance criteria, and governance mechanisms.

8 CONTEXT AND SCOPE

This stage involves gathering information and studying the external context (financial, economic, regulatory, socio-environmental environment and stakeholder relations) and the internal context (governance, organizational structure, strategy, processes, systems, contracts, audit reports and other available assessments). For scope definition, that is, critical activities and themes that will be mapped, thus arriving at the risk scenarios to be evaluated.

8.1 RISK IDENTIFICATION

8.1.1 Based on the results of the risk mapping, the risks that may impact Iguá in achieving its objectives are identified, as well as those responsible for them (Risk Owner).

8.1.2 To identify, recognize, and describe risks, the process is conducted based on the Company's risk portfolio (*LI-COR-RCI-001 – Iguá Corporate Risk Portfolio List)* , allowing for a structured analysis and detailed identification of risks and risk factors that directly impact the business. This approach ensures a comprehensive and strategic view, aligning risk management with corporate objectives.

8.2RISK CATEGORIZATION

8.2.1 For categorization purposes, Risks at Iguá should be divided as follows: Strategy, Regulatory and Litigation, Socio-environmental, Compliance and Reporting, Financial, Operational and Technology. **See Annex I.**

8.3RISK ANALYSIS (IMPACT AND PROBABILITY)

8.3.1 The Company's risk analysis is conducted through a combined assessment of impact and probability, with the objective of determining the level of risk exposure and supporting the prioritization of response actions. Impact represents the magnitude of the potential effects of risk on Strategic, Regulatory and Litigation, Socio-environmental, Compliance and Reporting, Financial, Operational and Technological objectives, and is measured based on predefined criteria. Probability corresponds to the chance of occurrence of the risk event,

considering the history of events, the control environment, the complexity of processes and relevant internal and external factors.

The combination of impact and probability levels results in the risk classification according to the risk matrix adopted by the Company, allowing its comparison with the Risk Appetite Ratio (RAS).

8.3.2 Risk analysis should determine the Level of Risk Exposure (High, Significant, Moderate , or Low), taking into account controls and initiatives implemented (residual risk).

8.3.3 The Company adopts as a premise the assessment of **corporate risks** in their residual condition, considering the existing environment of controls, processes, governance structures and management practices. This approach is aligned with COSO Enterprise Risk Management (ERM), which prioritizes the analysis of actual risk exposure in relation to strategic, operational, financial, regulatory and compliance objectives.

Direct assessment of residual risk allows for a more accurate view of the Company's effective exposure, supporting decision-making, alignment with Risk Appetite, and the appropriate definition of risk responses, such as accepting, mitigating, transferring, or avoiding.

For the purposes of corporate consolidation and reporting to senior management and governance bodies, the assessment of residual risk will be considered.

8.3.4 **Transactional risks** should be assessed in a structured way, considering two complementary dimensions: inherent risk and residual risk.

Risks should initially be assessed in their inherent condition, considering the nature, complexity, materiality, volume, and recurrence of transactions, as well as the degree of human judgment and applicable regulatory requirements. Subsequently, risks should be assessed in their residual condition, in light of the effectiveness of existing internal controls. The assessment of residual risk forms the basis for decisions regarding treatment, prioritization, approval, and escalation, and should be compared to the limits established in the Risk Appetite Assessment (RAS).

8.4RISK CLASSIFICATION AND MONITORING

8.4.1 The risk management process includes not only the identification of risks and risk factors, but also their classification and monitoring of their treatment. Thus, after analysis, the identified risks are classified as "High," "Significant," "Moderate," or "Low," with "High" and "Significant" risks being reported to Senior

Management and governance bodies as recurring agenda items in their ordinary or extraordinary meetings.

8.4.2 The classification is defined through the evaluation and application of a set of probability criteria (historical occurrence or estimated projection of the possible materialization of risk factors) and impact criteria (potential consequences arising from the occurrence of the risk), considering:

- Strategic planning and objectives;
- Parameters proportional to the size of the company, updated periodically;
- Comprehensive quantitative (not just financial) and qualitative vectors;
- Risk Appetite (defined by Management and the Board according to each specific risk); and
- Controls and mitigating initiatives (residual risk).

8.4.3 The detailed methodology and classification criteria, as well as the risk response and monitoring mechanisms, are in the procedure (*PR-COR-RCI-001 – Risk Management and Internal Controls Procedure),* which has been duly approved and adheres to market standards and best practices.

8.5 TREATMENT AND RESPONSE TO RISKS

8.5.1 The Business Areas are responsible for defining and implementing preventive and corrective actions to respond adequately and effectively to the Company's risks, adopting, as appropriate, the following response strategies: accepting, sharing or transferring, avoiding or reducing risks, in order to keep them within the limits of the established Risk Appetite. See Annex II.

8.5.2 At this stage, the best risk response options should be selected and implemented, the effectiveness of this response evaluated, a decision made on whether the remaining risk is acceptable, and, if applicable, additional treatments implemented. Benefits, costs, efforts, advantages, and disadvantages of implementation must be balanced. For example, it is possible to:

- Conduct further analyses for a better understanding of the risk;
- Enhance existing controls and initiatives and assess the need for new implementations;
- Insurance contract for risk sharing and monitored retention.

8.5.3 Any acceptance of risks of any nature must comply with the provisions of *PR-COR-RCI-003 - Risk Governance and Internal Controls Procedure* , applied to

the entire Company, including risks identified in internal audits and necessarily following the approval levels, as mentioned in the Company's Approval Levels Table (ALC-RCI-1: Acceptance of high and significant risks where the Company does not implement controls or mitigation initiatives).

8.6 EFFECTIVE DATE

8.6.1 The Corporate Risk Matrix (Iguá Sanitation and Operations) will be reviewed annually or promptly, when necessary.

8.6.2 The Transactional Risk Matrix will be reviewed annually during the current cycle or promptly, when necessary.

9 DUTIES AND RESPONSIBILITIES

9.1 COMPLIANCE, RISK AND INTERNAL CONTROLS MANAGEMENT

- To act as a second line of defense, ensuring integration between risk, internal controls, compliance, and governance.
- To establish, maintain, and safeguard the corporate methodology for risk management and internal controls, in alignment with COSO ERM, COSO ICIF, and IBGC best practices.
- Maintain up-to-date policies, procedures, and risk assessment criteria, including impact, probability, and risk appetite assessment (RAS) methodology.
- Consolidate, update, and report the Corporate Risk Matrix and the status of mitigation actions to the relevant governance bodies.
- To advise Risk Owners on the identification, assessment, treatment and monitoring of risks, including the definition of indicators.
- To monitor risk exposures, the adequacy of responses, and the effectiveness of associated internal controls.
- Define and coordinate the work plan and internal control tests related to corporate risks.
- To report, in a timely and objective manner, the main risks, exposures and test results to Senior Management and Governance bodies .
- To promote a culture of risk, internal controls, and compliance throughout the Company.

9.2 EXECUTIVE BOARD OF FINANCE AND INVESTOR RELATIONS (CFO)

- To define guidelines and strategies for risk management and internal controls.
- To assess and deliberate on the Risk Matrix and treatment strategies.
- To ensure the timely reporting of relevant changes in risk criticality to Senior Management and Governance bodies.
- To demand the mapping and treatment of new or significantly altered risks.
- Ensure the Risk Matrix is updated in light of strategic changes or relevant events.
- To supervise and request, when necessary, the review of the Risk Appetite Assessment (RAS).

9.3 AUDIT COMMITTEE (CAE)

- Validate and recommend improvements to the guidelines for the structure, governance, and process of Risk Management and Internal Controls.
- To oversee the structure and process of risk management and internal controls.
- Evaluate and monitor the Corporate Risk Matrix, the effectiveness and adequacy of the internal control structure, as well as preventive and mitigating actions, focusing on relevant risks.
- To propose and recommend the Risk Appetite Statement (RAS) to the Board of Directors.
- Recommend updates to the Risk Management Policy.
- Ensure timely reporting to the Board of Directors on relevant risk levels.
- Recommend the continuous improvement of risk governance.
- Report to the Board of Directors on the risk levels (high and significant).

9.4 BOARD OF DIRECTORS (BOD)

- Approve the Risk Management Policy and its revisions.
- To define and approve the Company's Risk Appetite Statement (RAS).
- To oversee the risk management system, ensuring its alignment with the business strategy and sustainability.
- Monitor relevant and critical risks, as well as exposures outside of the Risk Appetite.
- To ensure integration between strategy, risks, internal controls, and governance.
- Assess the adequacy of the risk governance structure, including resources, competencies, and independence of functions.

- Receive and analyze periodic reports from the Audit Committee and Management regarding risk management.

9.5 RISK OWNERS (BUSINESS AREAS)

- Identify, assess, and technically review the risks under your responsibility, including risk factors, causes, impacts, probability, and responses, in accordance with the corporate methodology.
- To define and execute action plans and responses to risks, coordinating, when necessary, the involvement of other areas to ensure adequate mitigation.
- Continuously monitor the risks under your management, through the development and monitoring of associated indicators and controls.
- Report periodically to the Compliance, Risk and Internal Controls area on the progress of mitigation actions and the evolution of risk exposure.
- Reassess the risk whenever there are relevant changes in the context, probability, impact, or operating conditions.
- Promptly communicate any significant changes to established risks, controls, initiatives, or action plans to the Compliance, Risk, and Internal Controls area.

10 APPROVAL LEVEL

The Corporate Risk Matrix, which consolidates risks of a strategic and corporate nature, is submitted to the Executive Board for approval. The Transactional Risk Matrix, which includes operational risks and internal controls associated with processes and transactions, is approved by the Business Area Management, observing the established levels of authority and criteria.

The approval levels for the Risk and Internal Controls area are formalized in the Approval Levels Table available in the Company's system as follows:

- ALC-RCI-1: Acceptance of high and significant risks.
- ALC-RCI-2: Governance for reprogramming risk mitigation action plans.
- ALC-RCI-3: Validation and approval of corporate risks.
- ALC-RCI-4: Validation and approval of transactional risks.

11 APPENDICES

- Annex I – Risk Categorization
- Annex II – Treatment and Responses to Risk
- MP-COR-RCI-001 – Map of the Sanitation Value Chain – Iguá.

ANNEX I

RISK CATEGORIZATION

Category	Description
Strategy	These are the risks associated with management decision-making that can lead to substantial losses in the company's economic value. Furthermore, they can negatively impact the company's revenue or capital as a result of inefficient planning, adverse decision-making, and changes in its business environment. Potential impact arising from decisions, investments due, and lack of responsiveness to changes in the environment.
Regulatory and Litigation	Risks related to compliance with applicable legislation in the area of operation, as well as general laws (environmental, labor, civil and tax/fiscal) and non-compliance with the Iguá Group's concession contracts. Potential impact resulting from non-compliance with laws or regulations or lawsuits filed by clients or counterparties. Risks related to compliance with regulatory standards that may lead to legal sanctions, interruption of activities, loss of licenses and damage to institutional reputation.
Socio-environmental	Risks of losses in the Company's results and balance sheet, caused by direct or indirect damage to the environment. Potential impact resulting from an event associated with inadequate management of socio-environmental issues.
Compliance and Reporting	Risks related to integrity, the absence of an effective compliance structure compromising credibility, deterring investments, and exposing the Company to fines and penalties. Misconduct, unethical acts or fraud, corruption and bribery, harassment and discrimination, conflicts of interest resulting in financial impacts and negative image and reputational damage. Reporting of unreliable or misleading financial statements, strategic misalignment in the definition of goals and indicators, represent severe risks to the transparency, credibility, and sustainability of the Company.
Financial	Risk of loss of financial resources by the Company related to foreign exchange exposures, interest rates and price fluctuations (e.g., lack of adequate approval processes, lack of transaction reconciliation, foreign currency operations, commodity prices, reduction in contribution margin, unauthorized access to system transactions, etc.).
Operational	Operational loss risks stem from inadequate internal processes, technological failures, human or system errors, and also include environmental, social, and operational fraud risks. These risks are directly linked to the Company's infrastructure, encompassing processes, people, and technology, and impact operational efficiency as well as the effective use of available resources. Operational problems, such as failures in internal

	controls, can lead to legal and regulatory sanctions, in addition to jeopardizing business continuity.
Technology	Risks that consist of the loss, misuse, unauthorized access, or disclosure of personal information or data of internal or external stakeholders, which may threaten the business or damage the Company's image, impacting financial losses and even business continuity.

ANNEX II

TREATMENT AND RESPONSE TO RISKS

Risk Response	Description
To accept	This strategy is adopted when it is not possible or practical to respond to the risk using other strategies. When Senior Management decides to accept the risk, it means they are agreeing to face the risk if and when it occurs. An emergency contingency plan or a fallback plan should be developed for this eventuality.
Share/Transfer	It involves finding another party willing to assume responsibility and bear the impacts of the risk, should it occur (e.g. , insurance, bonds, and guarantees).
Avoid	Risk can be avoided by removing the cause of the risk or by performing the operation in a different way, while still remaining in line with achieving the Company's objectives. Not all risks can be avoided/eliminated, and this approach can be costly.
Reduce / Decrease	Risk mitigation reduces the probability and/or impact of an adverse risk event to an acceptable limit (expected residual risk) through the implementation of controls and initiatives. The implementation of controls and/or initiatives can occur immediately or within defined timeframes through established action plans.